What is claimed is:

1. An optical media storage device of a selected format that is adapted to be read by and optical reader, comprising:

(a) a substrate having a first surface and an opposite second surface, said first surface having a data structure formed thereon which includes:

an anomaly region configured to generate one or more errors when read by the optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a hashing algorithm; and

a program region having informational pits and lands corresponding to an executable application program which incorporates said hashing algorithm, said application program being coded such that, when said optical media storage device is read by the optical reader, said hashing algorithm is executed against said anomaly region to generate a test hash value;

(b) a metallic reflective layer disposed over said data structure; and

(c) a protective layer disposed over said metallic reflective layer.

2. An optical media storage device according to claim 1 wherein said application program is operative to execute improperly if said test hash value is different than the target hash value.

3. And optical media storage device according to claim 1 wherein said hashing algorithm is MD-5.

4. An optical media storage device according to claim 3 wherein said target hash value is a 128-bit key.

5. An optical media storage device according to claim 1 wherein said hashing algorithm is obscured within said application program.

6. An optical media storage device according to claim 1 wherein said anomaly region, said fingerprint region and said executable region reside at separate locations on said substrate.

7. An optical media storage device according to claim 1 wherein optical media device is of a CD-ROM format.

8. An optical media storage device according to claim 1 wherein said substrate comprises polycarbonate and said protective layer is a polymeric film.

9. An optical media storage device according to claim 1 wherein said anomaly region comprises a plurality of contiguous physical defects formed on said substrate.

10. An optical media storage device according to claim 1 wherein said anomaly region comprises a plurality of anomalies formed on said substrate which have characteristics falling outside of normal operating specifications for the selected format.

11. An optical media storage device according to claim 1 wherein the informational pits and lands associated with said fingerprint region are contiguous.

12. In a multi-layer optical media storage device of a selected format that is adapted to be read by an optical reader, wherein optical media storage device comprises a polycarbonate substrate, a metallic reflective layer disposed over said substrate, and a polymeric film disposed over said metallic reflective layer, the improvement comprising a data structure formed on said substrate which includes:

an anomaly region configured to generate one or more predictable errors when read by the optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a hashing algorithm; and

a program region having associated informational pits and lands corresponding to an application program which incorporates said hashing algorithm.

13. The improvement of claim 12 wherein said application program is coded to scan said anomaly region and apply results obtained from said scan as an input to said hashing algorithm in order to generate a test hash value, said application program being further coded to execute improperly if said test hash value is different than the target hash value.

14. The improvement of claim in 12 wherein said hashing algorithm is selected from a group consisting of MD-2, MD-4, MD-5 and SHA-1.

15. The improvement of claim 14 wherein said hashing algorithm is obscured within an executable form of said application program.

17. The improvement of claim 12 wherein each of said anomaly region, said fingerprint region and said executable region resides at an unique location on said substrate.

18. The improvement of claim 12 wherein said anomaly region comprises a plurality of contiguous physical defects formed on said substrate.

19. An optical media storage device according to claim 12 wherein said anomaly region comprises a plurality of anomalies formed on said substrate which have characteristics falling outside of normal operating specifications for the selected format.

20. A method of manufacturing a copy protected optical media storage device, comprising:

(a) creating a mastering tape having information corresponding to a data structure to be formed on a substrate, wherein said data structure is to include:

an anomaly region configured to generate one or more predictable errors when read by an optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a selected hashing algorithm; and

a program region having associated informational pits and lands corresponding to an application program which is coded to execute said hashing algorithm against said anomaly region to generate a test hash value, and to abort normal program operation if said test hash value does not match said target hash value;

(b) generating a glass master from said mastering tape;

(c) fabricating at least one stamper suitable for injection molding from said glass master;

(d) molding a polycarbonate substrate from said stamper;

(e) coating said polycarbonate substrate with a metallic reflective layer; and

(f) forming a protective layer over said metallic reflective layer.

21. A method of assessing authenticity of optical media, comprising:

(a) providing an optical media storage device comprising:

(i) a substrate formed to include a data structure having:

an anomaly region configured to generate one or more predictable errors when read by an optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a hashing algorithm; and

a program region having informational pits and lands corresponding to an application program which incorporates said hashing algorithm, said application program being coded such that, when said optical media storage device is read by the optical reader, said hashing algorithm is executed against said anomaly region to generate a test hash value;

(ii) a metallic reflective layer disposed over said data structure; and

(iii) a protective layer disposed over said metallic reflective layer;

(b) reading said optical media storage device with an optical reader whereby said hashing algorithm is executed against said anomaly region thereby to generate said test hash value; and

(c) authenticating said optical media only if said test hash value matches said target hash value.

22. A method according to claim 21 whereby normal operation of said application program is aborted if the test hash value does not match the target hash value.

23. A method according to claim 21 said hashing algorithm obscured within said application program and is selected from a group of algorithm's consisting of MD-2, MD-4, MD-5 and SHA-1.